iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review Paper on Image Steganography and its Techniques

Ms. Tejal[1], Mr. Divyanshu Rao[2]
[1,2]Department of Electronics and Communication, Shri Ram Institute of Technology, Jabalpur M. P.

Abstract: ***Steganography is an important field of research in recent years involving a number of applications in real world. It is the method of embedding information into the image file without causing statistically significant modification to the original image. The present task is to transferring the embedded information using image steganography to the destination without being detected. This paper describes the hiding data in an image file using Discrete Wavelet Transform (DWT), Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and based steganography. The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the LSB of cover image to derive the stego-image whereas DCT & DWT algorithm are implemented in frequency domain in which the stego -image is transformed from spatial domain to the frequency domain and the payload bits are embedded into the frequency components of the cover image files. The performance of these methods are analyzed on the basis of the parameters Mean square error (MSE) and peak signal to noise ratio (PSNR).***

Keywords : Steganography, Mean square error (MSE) , peak signal to noise ratio (PSNR) least significant bit (LSB), discrete cosine transform (DCT), discrete wavelet transform (DWT).

I. INTRODUCTION

In the present year, high secure and information hidden based communication is the foremost requirement of the users those who have used different communication sources for secret transmission . Therefore steganography is the main approach by people due to the security issues over internet. Steganography is methods in which a hiding a file or information in some form of image, audio and video formats. The main objective of steganography is hiding the embedded information into the cover image file. There are different techniques to implement steganography approach these methods are least significant bit (LSB), discrete cosine transform (DCT) and discrete wavelet transform(DWT) technique. In steganogrphy there are two types of domains in which cover image is implemented i.e. spatial domain & frequency domain [6]. In spatial domain, processing is applied directly on the pixel values of the image whereas in frequency domain, pixel values are transformed and then Processing is applied on the transformed coefficients.

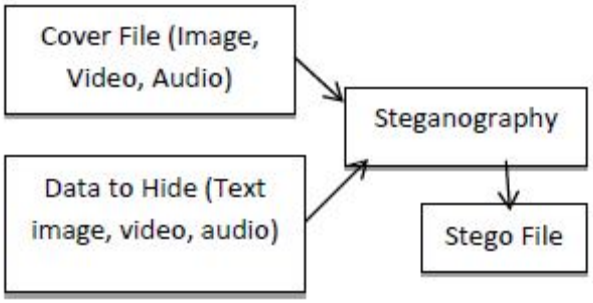


Figure 1: Steganography implementation.

Least significant bit technique is processed in spatial domain while DCT & DWT technique are implemented in frequency domain. In least significant bit (LSB), each pixel of an image transformed into the binary value and data is hidden into the least significant position of the binary value of the pixels of the image in such a manner that, it doesn't destroy the integrity of the cover image but this scheme is sensitive to a variety of image processing attacks like compression, cropping etc. To transforming the digital image data from the spatial to the frequency domain used DCT, which is used after transforming the image into the frequency domain. The discrete cosine transforms (DCT) & discrete wavelet transform (DWT) are mathematical function, the data is embedded in the least

significant bits of the medium frequency components and is specified for lossy compression while In DWT, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform and provide maximum robustness.

II. LITERATURE SURVEY

J.R. Krenn explained steganography and its implementation techniques [1] et. al. proposed the LSB embedding technique explained that the data can be hidden in the LSB of the cover image and the human eye would be unable to identified the hidden image in the cover image. This paper proposed the least significant bit and embedding technique which presents the results for two, four and six bit Leas LSB for a .png file and a .bmp file [2]. K.B. Raja, et. al. Explained the transferring the embedded information into the final destination without being detected or in simply without being hacked. In this paper, the image based steganography that conatins Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and compression techniques on basic images to enhance the security of the payload data [3]. Sharma, et. al. has proposed a new steganography algorithm for eight bits (gray scale) or twenty four bits (color image) based on logical operation to ensure the security against the steganalys is attack on the information's[4]. Po-Yueh Chen, et. al. proposed a advance steganography methods which provides the secret messages in frequency domain. According to different peoples demands on the secret information capacity and image file, this proposed algorithm of this paper is divided into two different modes and five different events[5]. Chen Ming, et. al. explain on the steganography algorithms based on this research, these tools are sepearted into five categories: (1). Spatial domain based tools; (2). Transform domain based tools; (3). Document based tools; (4) File structure based tools; (5) other categories, e.g. video compress encoding and spread spectrum technique based tools[6]. Aneesh Jain, et. al. describes a methods which hides text information in bitmap images format, in this scheme there is almost no perceptible difference between the original image and this new embedded image and which is also resistant to JPEG compression techniques[7]. Mehboob, et. al. Worked on the Steganography in general and proposes a advanced technique to hide data in a colourful image using least significant bit technique[8]. Mathkour, et. al. Describes the recent techniques and a more robust steganography technique has been proposed that takes many advantages of the strengths and avoids the limitations in the data hiding[9]. Rao Thota, et. al. explained and implement the basic JPEG compression using only basic MATLAB functions in stegnogrpahy[10]. Mamta Juneja, et. al. proposed the design of a image steganography technique based on LSB and using RSA encryption technique for secure encryption[11]. K.B. Kumar, et. al. explained in his paper the main issue of present communication is establishing secret communication over the channel while using the public channel and is achieved by steganography tool [12]. Dr. Walia, et. Al this paper explained the analysis of Least Significant Bit (LSB) based Steganography with Discrete Cosine Transform (DCT) based Steganography techniques [13]. K Suresh Babu, et. al. defined an image Steganography method that can fulfil the recruitment and reliability of the hidden data that being transmitted to the receiver in network. The method can also fulfil whether the attacker has tried to hack secret information in the stego-image [14]. T. Narasimmalou, et. al. Explained an optimal discrete wavelet transform (DWT) based steganography for high security. This experiments show that the peak signal noise ratio (PSNR) generated by the proposed method is better than the previous work[19].

III. METHODS OF CONCEALING DATA IN DIGITAL IMAGE

Steganography is used for the data hiding communication or as we can say for the secure communication where secret image which is communicated to the destination is embedded into the cover image to derive the stego image. In this section we proposed the embedding and retrieval techniques which are :

A. Least Significant Bit Substitution Technique (LSB)

In the LSB steganography the simplest form of the LSB steganogrphy is to replace the LSB for the digital image file. LSB steganography technique converts the last bit of each of the data values in the message that used to be hidden. Consider an Eight-bit grayscale bitmap image file where each pixel is stored as a byte representing a gray scale value suppose the first eight pixels of the original image have the following gray scale values [4]:

11010010
01001010
10010111
10001100
00010101
01010111

00100110
01000011
The character C whose binary value is 10000011 to hide the letter, we would replaced the LSBs of these pixels to have the following new gray scale values:
11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011
Note that, on average, only half the LSBs required to change. The difference between the original (i.e. cover) image and the stegno image will be very difficult to notice for the human eye. However, there is one of its major limitations is small size of data which can be embedded in stegno images using only LSB methods. LSB is extremely vulnerable to attacks during transmission. LSB techniques implemented to 24 bit formats are difficult to identify contrary to 8 bit formats [8].

B. Discrete Cosine Transform Technique (DCT)

JPEG compression technique is used in DCT coefficients [10][12]. It divides the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can divides the image into high, middle and low frequency components. In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks [13]. So the secret information's are embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. The general equation for a 1D (N data items) DCT is defined by the following equation: [12] be affected.

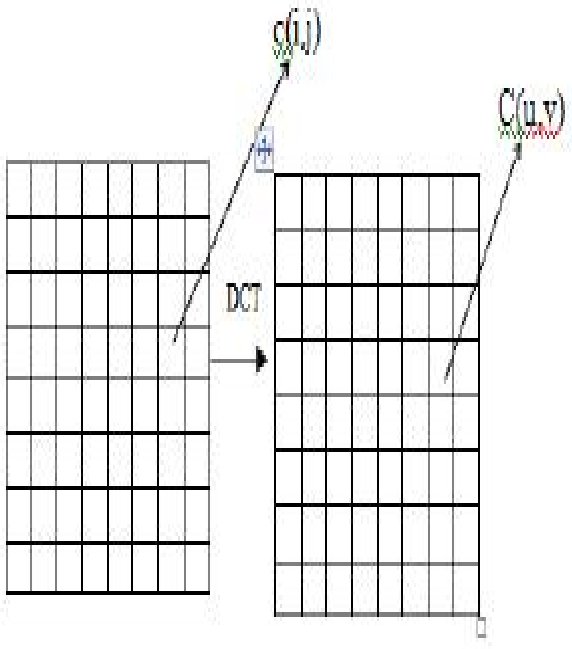


Figure 2: DCT of an Image

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

$$C(u) = a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where u= 0, 1, 2..... N-1

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:[12]

$$C(u,v) = a(v)\sum_{i=0}^{N-1}[a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)] \times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

Where u, v = 0, 1, 2....N-1

Here, the input image is of size N X M. c (i, j) is the intensity of the pixel in row i and column j; C (u,v) is the DCT coefficient in row u and column v of the DCT matrix[11].

DCT is used in steganography as [10]- Image is broken into 8×8 blocks of pixels parts. In DCT the working is done from left to right, and top to bottom, also DCT is applied to each and every block of the image file. Each block of images is compressed through quantization table to scale the DCT coefficients and information is embedded in DCT coefficients.

C. Discrete Wavelet Transform Technique (DWT)

There are two operations performed in a 2-dimensional Haar-DWT: Horizontal and other is the vertical. The detailed techniques of 2-D Haar-DWT are described as follows:

Step I: At first step the scan image pixels starts from left to right direction in horizontal way. Then, perform the addition and subtraction mathematical operations on neighbouring pixels. Keep save the sum value on the left and the difference value on the right as illustrated in Figure 3. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

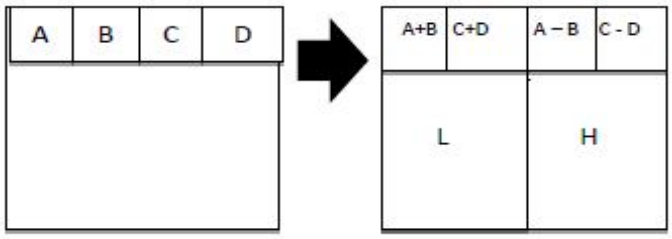


Figure 3: Horizontal operation

Step II: Secondly, scan the pixels from top to bottom in vertical direction. perform the mathematical addition and subtraction operations on neighbouring pixels of image and then keep save the sum value on the top and the difference value on the bottom as illustrated in Figure 4. Repeat this steps until all the columns are processed. Finally we will get 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency part and hence looks very similar to the original image. The whole procedure is known as the first-order 2-D Haar-DWT.

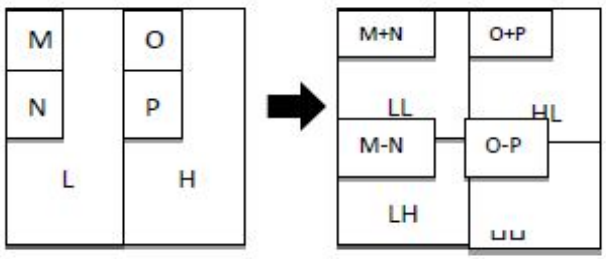


Figure 4: Vertical operation.

IV. CALCULATION OF IMAGE QUALITY

For analysing and comparing stegno image with cover image results it requires a measure of image quality, commonly used measures are Mean-Squared Error(MSE), Peak Signal-to- Noise Ratio(PSNR) and capacity.

A. *Mean-Squared Error*

The mean-squared error (MSE) between two images I1 (m,n) and I2(m,n) is [2]:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N}$$

M and N are the number of rows and columns in the input images, respectively.

B. *Peak Signal-to-Noise Ratio*

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image Range [5]:

$$PSNR = 10 \log_{10} \frac{256^2}{MSE}$$

PSNR is measured in decibels (dB). PSNR is a evaluating measure for comparing and for restoration results for the same covering image.

C. *Capacity*

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. In the steganography for hiding information, operation needs to stroe the statistical properties of the cover image in addition to its quality. Therefore capacity depends on total number of bits per pixel & number of bits embedded in each pixel. Capacity is explained by bits per pixel (bpp) for image and the Maximum Hiding Capacity (MHC) in terms of its percentage value [13].

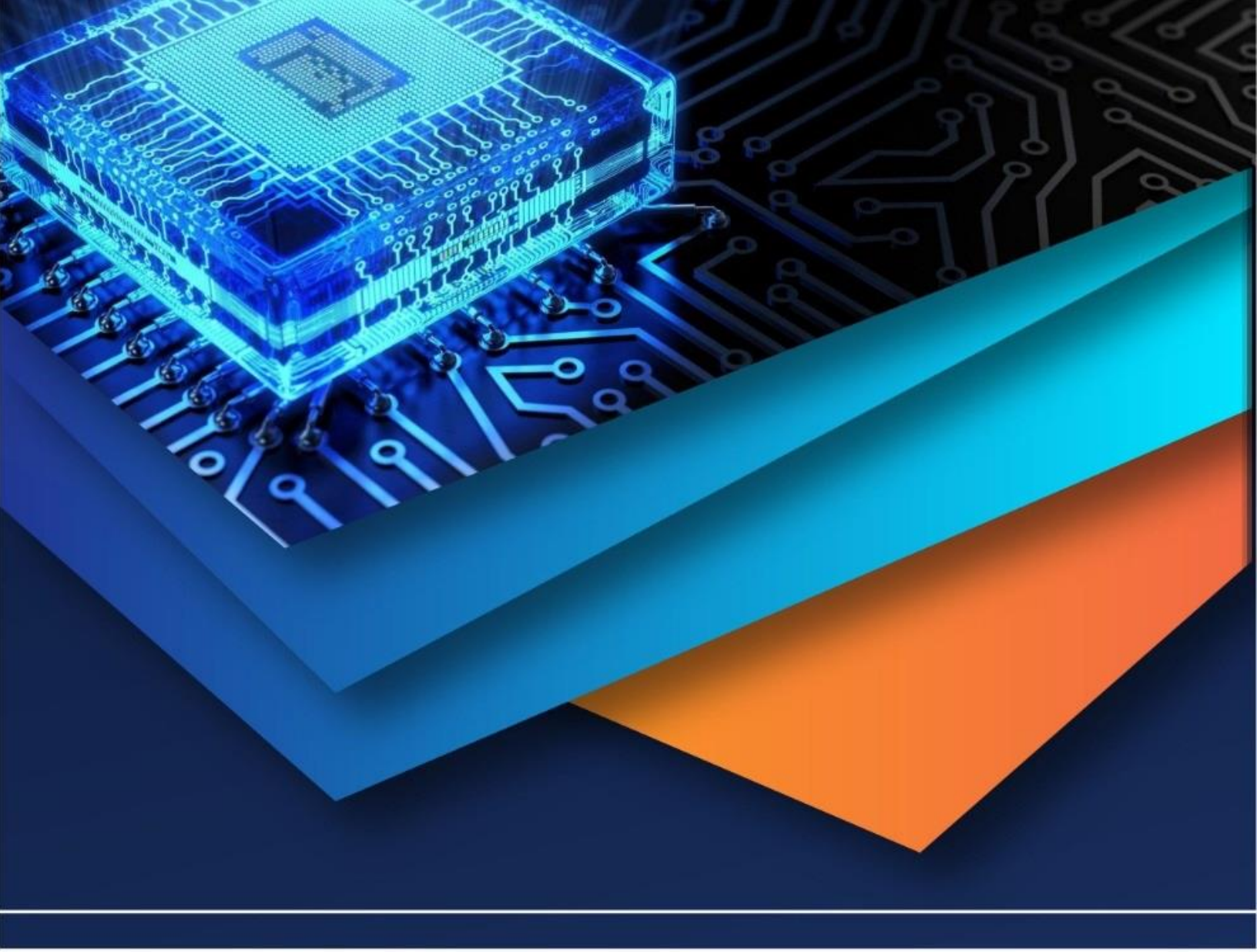
V. CONCLUSION

Steganography is the process where hidden information or messages is embedded into the cover image file and only sender or transmitter and receiver can read that hidden data or message. It is emerging in its peak because it does not attract anyone by itself [24]. In this paper, analysed the least significant bit, discrete cosine transform & discrete wavelet transform methods has been successfully implemented and results are evaluated. The MSE and PSNR of the methods are also compared and also this paper presented a background discussion and implementation on the major algorithms of steganography deployed in digital imaging. The peak signal to noise ratio describes the image quality after hiding or embedded the data into the cover image. This shows that DCT provides high quality of the image. An embedding algorithm is said to br reliable if the embedded or hidden message or data can be extracted after the image has been manipulated without being destroyed or any noise or loss. DWT is a highly robust and efficient method in which the image is not changes is sized so much when we hides our information and this methods provides so much security as compared to others transformations.

REFERENCES

[1] J.R. Krenn, “Steganography and Steganalysis”, January 2004.
[2] Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs, “Implementation of LSB Steganography and its Evaluation for Various Bits”, 2004.
[3] K.B. Raja, C.R. Chowdary, Venugopal K. R, L.M. Patnaik, “A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images”, IEEE-0-7803-9588-3/05/$20.00 ©2005.
[4] Vijay Kumar Sharma, Vishalshrivastava, “A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection.” Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.
[5] Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.
[6] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, “Analysis of Current Steganography Tools: Classifications & Features”,International Conference on Intelligent Information Hiding and Multimedia signal Processing (IIH-MSP'06),IEEE- 0-7695-2745-0/06 $20.00 © 2006.
[7] Aneesh Jain, Indranil Sen. Gupta, “A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images”,IEEE-1-4244-1272-2/07/$25.00©2007.
[8] Beenish Mehboob and Rashid Aziz Faruqui, “A Steganography Implementation”, IEEE -4244-2427- 6/08/$20.00 ©2008.
[9] Hassan Mathkour, Batool Al-Sadoon, Ameur Touir, “A New Image Steganography Technique”, IEEE- 978-1-4244-2108-4/08/$25.00 © 2008.
[10] Nageswara Rao Thota, Srinivasa Kumar Devireddy, “Image Compression Using Discrete Cosine Transform”, Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[11] Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.
[12] Dr. EktaWalia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.
[13] K.B. Shiva Kumar, K.B. Raja, R.K. Chhotaray, Sabyasachi Pattnaik, "Coherent Steganography using Segmentation and DCT", IEEE-978-1-4244- 5967-4/10/$26.00 ©2010.
[14] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication of Secret Information in Image Steganography" .
[15] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887), Volume 9, No.7, November 2010.
[16] Atalla I. Hashad, Ahmed S. Madani, "A Robust Steganography Technique Using Discrete Cosine Transform Insertion".
[17] Vijay Kumar, Dinesh Kumar, "Performance Evaluation of DWT Based Image Steganography", IEEE- 978-1-4244-4791-6/10/$25.00_c 2010.
[18] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
[19] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based steganography", IEEE International Conference on Advanced Communication Control and Computing Technologies(ICACCCT),2012.
[20] Neda Raftari and Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCTIWT", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.
[21] Ankita Sancheti, "Pixel Value Differencing Image Steganography Using Secret Key" International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-2, Issue-1 and December 2012.
[22] Neha Batra & Pooja Kaushik, "Implementation of Modified 16×16 Quantization Table steganography on Color Images", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 10, October 2012.
[23] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", proceedings of international multi conference of engineers & computer science, IMECS-Volume I,March 16-18, 2011.
[24] Gurmeet Kaur and Aarti Kochhar, "A Steganography Implementation based on LSB & DCT", International Journal for Science and Emerging, Technologies with Latest Trends" 4(1), ISSN No. Online): 2250-3641, ISSN No. (Print): 2277-8136, 35-41 (2012).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY